(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 07200433 A

(43) Date of publication of application: 04.08.95

(51) Int. Cl G06F 13/00
H04L 12/66

(21) Application number: 06012099

(22) Date of filing: 07.01.94

(71) Applicant: FUJI FACOM CORP

(72) Inventor: SHIROKURA YOSHIZUMI

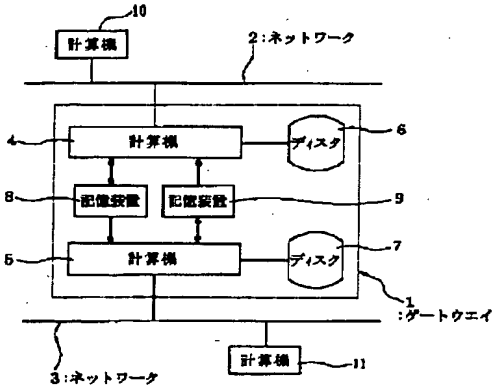
(54) GATEWAY

(57) Abstract:

PURPOSE: To improve the security by preventing illegal invasion among networks.

CONSTITUTION: A couple of storage devices 8 and 9 where writing in mutually opposite directions is restricted are provided, and transfer data sent from a computer 10 to a computer 4 are written in the storage device 8. A computer 5 takes data out of the storage device 8 and sends them to a computer 11 at a transfer destination. Flag data for erasing data in the storage device 8 which are already processed by the computer 4 are generated by the computer 5 and written in the storage device 9. The computer 4 erases the object data in the storage device 8 on the basis of the flag data in the storage device 9. Then the computer 5 checks whether or not the data corresponding to the flag data are erased and then erases the flag data on condition that the data have been erased.

COPYRIGHT: (C)1995,JPO



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平7－200433
(43)公開日　平成７年(1995)８月４日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　13/00	３５３　Ｃ	7368－5B		
Ｈ０４Ｌ　12/66				
		8732－5K	Ｈ０４Ｌ　11/ 20	Ｂ

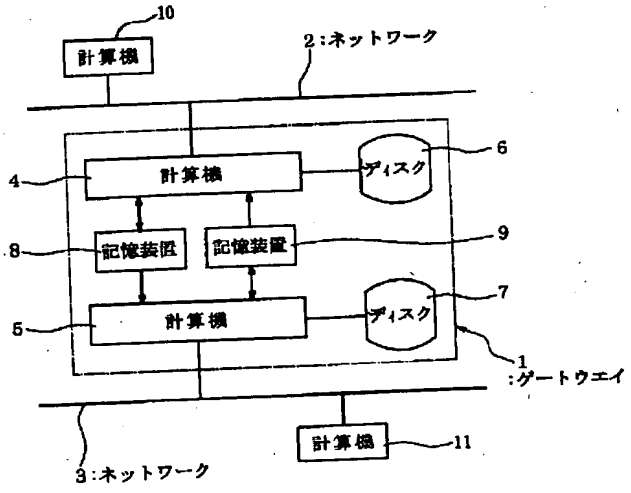
審査請求　未請求　請求項の数１　ＦＤ　（全４頁）

(21)出願番号　特願平6－12099
(22)出願日　平成６年(1994)１月７日

(71)出願人　000237156
富士ファコム制御株式会社
東京都日野市富士町１番地
(72)発明者　白倉　善積
東京都日野市富士町１番地　富士ファコム制御株式会社内
(74)代理人　弁理士　森田　雄一

(54)【発明の名称】　ゲートウエイ

(57)【要約】
【目的】　ネットワーク間の不法侵入を防止してセキュリティを高める。
【構成】　互いに反対方向の書込みを制限した１対の記憶装置８，９を備えておき、計算機１０から計算機４へ送られた転送データを記憶装置８へ書き込む。計算機５は記憶装置８内のデータを取り出して転送先の計算機１１へ送信する。記憶装置８内の処理済みのデータを計算機４により消去するためのフラグデータを、計算機５が作成して記憶装置９内に書き込む。計算機４は、記憶装置９のフラグデータに基づき記憶装置８内の消去対象データを消去する。次に、計算機５はフラグデータに対応するデータが消去されたか否かを調べ、消去されていればそのフラグデータを消去する。



1

【特許請求の範囲】

【請求項１】　それぞれのネットワークごとに設置された転送データメモリと、

両ネットワークの間に設置されて両ネットワーク側からのリード・ライトが可能な共有メモリと、

それぞれのネットワークごとに設置され、送信先が他のネットワークである転送データを自ネットワークから受信して転送データメモリに格納する手段と、

それぞれのネットワークごとに設置され、転送データメモリに格納されている転送データを読み取り共有メモリに書き込む手段と、

それぞれのネットワークごとに設置され、共有メモリに書き込まれている自ネットワーク宛の転送データを読み取り自ネットワーク上の送信先へ送信する手段と、

を備えたゲートウエイにおいて、

前記共有メモリを、一方のネットワーク側からはリードライトを可能としかつ他方のネットワークからはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワークからはリードオンリとした共有メモリとにより構成するとともに、

それぞれのネットワークごとに設置され、転送データが読み取られて送信された後にリードオンリの共有メモリに残った転送データを消去するためのフラグデータを作成してリードライト可能な共有メモリに書き込む手段と、

それぞれのネットワークごとに設置され、リードオンリの共有メモリに書き込まれているフラグデータに基づきリードライト可能な共有メモリに書き込まれている転送データを消去する手段と、

それぞれのネットワークごとに設置され、リードライト可能な共有メモリとリードオンリの共有メモリを比較して、リードライト可能な共有メモリに書き込まれているフラグデータに該当する転送データがリードオンリの共有メモリにない場合は、そのフラグデータをリードライト可能な共有メモリから消去する手段と、

を備えたことを特徴とするゲートウエイ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ゲートウエイに関し、詳しくは異なるネットワーク間でのリモートアクセスを不可能にしてセキュリティを高めたゲートウエイに関する。

【０００２】

【従来の技術】従来のゲートウエイは異なるネットワーク間に共通な記憶装置を設けて、相互間のデータ転送を行っている。

【０００３】

【発明が解決しようとする課題】しかしながらこれら従来のゲートウエイでは、ソフトウエアの設定を誤ると、

2

一方のネットワークの端末が保持する秘密情報を他方のネットワークの端末に転送可能な場合が発生するという問題があった。本発明は上記問題点を解決するためになされたもので、その目的とするところは、ネットワーク間のセキュリティを高めて、秘密情報が誤ってゲートウエイを通過して他のネットワークに転送されることのないようにしたゲートウエイを提供することにある。

【０００４】

【課題を解決するための手段】上記目的を達成するために、本発明は、それぞれのネットワークごとに設置された転送データメモリと、両ネットワークの間に設置されて両ネットワーク側からのリード・ライトが可能な共有メモリと、それぞれのネットワークごとに設置され、送信先が他のネットワークである転送データを自ネットワークから受信して転送データメモリに格納する手段と、それぞれのネットワークごとに設置され、転送データメモリに格納されている転送データを読み取り共有メモリに書き込む手段と、それぞれのネットワークごとに設置され、共有メモリに書き込まれている自ネットワーク宛の転送データを読み取り自ネットワーク上の送信先へ送信する手段とを備えたゲートウエイにおいて、前記共有メモリを、一方のネットワーク側からはリードライトを可能としかつ他方のネットワークからはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワークからはリードオンリとした共有メモリとにより構成するとともに、それぞれのネットワークごとに設置され、転送データが読み取られて送信された後にリードオンリの共有メモリに残った転送データを消去するためのフラグデータを作成してリードライト可能な共有メモリに書き込む手段と、それぞれのネットワークごとに設置され、リードオンリの共有メモリに書き込まれているフラグデータに基づきリードライト可能な共有メモリに書き込まれている転送データを消去する手段と、それぞれのネットワークごとに設置され、リードライト可能な共有メモリとリードオンリの共有メモリを比較して、リードライト可能な共有メモリに書き込まれているフラグデータに該当する転送データがリードオンリの共有メモリにない場合は、そのフラグデータをリードライト可能な共有メモリから消去する手段とを備えたことを特徴とする。

【０００５】

【作用】本発明においては、ゲートウエイの共有メモリが、一方のネットワーク側からはリードライトを可能としかつ他方のネットワークからはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワークからはリードオンリとした共有メモリとにより構成される。それぞれのネットワークごとに、転送データが読み取られて転送データメモリに書き込まれた後に、リードオンリの共有メモリに残った転送データを消去するためのフラグデータが作

成されてリードライト可能な共有メモリに書き込まれる。

【０００６】それぞれのネットワークごとに、リードオンリの共有メモリに書き込まれているフラグデータに基づきリードライト可能な共有メモリに書き込まれている転送データが消去される。それぞれのネットワークごとに、リードライト可能な共有メモリとリードオンリの共有メモリが比較され、リードライト可能な共有メモリに書き込まれているフラグデータに該当する転送データがリードオンリの共有メモリにない場合は、そのフラグデータがリードライト可能な共有メモリから消去される。これら手順により、ネットワーク間ではデータの転送方向に応じて異なる共有メモリを介してデータ転送がなされることにより、一方のネットワークの端末から他方のネットワークの端末に対してリモート・アクセスすることが不可能になる。

【０００７】

【実施例】以下、図に沿って本発明の実施例を説明する。図１は本発明の実施例を示すブロック図である。図において、１はゲートウエイであり、異なるネットワーク２，３の間に接続されている。ゲートウエイ１は、計算機４，５、転送データメモリであるところのディスク６，７、共有メモリであるところの記憶装置８，９から構成されている。記憶装置８は計算機４からのリード／ライト（ＲＷ）が可能であり、計算機５からはリードオンリ（ＲＯ）である。同じく、記憶装置９は計算機５からのリード／ライト（ＲＷ）が可能であり、計算機４からはリードオンリ（ＲＯ）である。

【０００８】次に、ネットワーク２上の端末である計算機１０から、ゲートウエイ１を介してネットワーク３上の端末である計算機１１へデータ転送する場合について説明する。先ず、計算機１０から転送先情報を付加した転送データがネットワーク２を介して、ゲートウエイ１内の計算機４へ送られる。計算機４は送られた転送データをいったんディスク６へ格納する。次に、計算機４は一定間隔で起動される監視プログラムにより、ディスク６を調べ、転送すべきデータがある場合は、そのデータを転送先情報とデータ本体の２つに分けて記憶装置８へ移動し、移動完了後にディスク６内のデータを削除する。

【０００９】一方、データを受け取る計算機５は、一定間隔で起動される監視プログラムにより、記憶装置８内を調べ、処理すべきデータがある場合は、記憶装置８からデータとその制御データを読み取り制御データ内に記述されている転送先である計算機１１へネットワーク３を介して送信する。ここまでは従来のゲートウエイとほぼ同様なデータ転送手順である。しかし、記憶装置８が計算機５からはリードオンリであるため、計算機５に転送データが読み取られても、消去されることがない。そのため、ネットワーク２からデータが転送されてくるたびに記憶装置８には処理済みの転送データが増えてしまう。

【００１０】そこで、記憶装置８内の処理済みのデータを計算機４により消去してもらうことを依頼するためのフラグデータを計算機５が作成して記憶装置９内に書き込む。計算機４は記憶装置９を監視しフラグデータがある場合は、そのフラグデータに基づき消去対象データが記憶装置８内にあるか否かを調べ、ある場合はそのデータおよび対応する制御データを消去する。次に、記憶装置９に残った使用済みのフラグデータを消去するため、計算機５は監視プログラムにより、記憶装置９にあるフラグデータに対応するデータおよび対応する制御データが記憶装置８内にあるか否かを調べ、ない場合はそのフラグデータは用済みであるので消去する。これら一連の処理により、記憶装置８内の転送済みの不要データが逐次消去されて、次のデータの書き込みエリアが確保される。

【００１１】なお、ネットワーク３上の計算機１１からゲートウエイ１を介してネットワーク２上の計算機１０へデータ転送をしようとする場合は、上述した手順を逆方向に実行することにより同様に転送される。このゲートウエイ１は、上述したように、データの転送方向によって、ネットワーク２，３間を接続する記憶装置８と記憶装置９のいずれかを限定して使用するため、一方のネットワークの計算機から他方のネットワークの計算機に対してのリモート・アクセス（リモート・コピー、リモート・シェルの実行等）を不可能にしてネットワーク経由の不法侵入を防止し、ネットワーク間のセキュリティを向上することができる。

【００１２】

【発明の効果】以上述べたように本発明によれば、共有メモリを一方のネットワーク側からはリードライトを可能としかつ他方のネットワークからはリードオンリとした共有メモリと、他方のネットワーク側からはリードライトを可能としかつ一方のネットワークからはリードオンリとした共有メモリとにより構成して、データの転送方向に応じて異なる共有メモリを介してデータ転送が行われる。それにより、一方のネットワークの端末から他方のネットワークの端末に対してリモート・アクセスすることが不可能となり、ネットワーク経由の不法侵入が防止されてネットワーク間のセキュリティが向上する。

【図面の簡単な説明】

【図１】本発明の実施例の構成を示すブロック図である。

【符号の説明】

１　ゲートウエイ
２，３　ネットワーク
４，５　計算機
６，７　ディスク
８，９　記憶装置

5　　6

１０，１１　計算機

【図１】